DDoS - bezpečnost, reálné zkušenosti

Futuretec 2023 - Ladislav Růžička

DoS,DDoS

- co je DoS a proč ho někdo dělá

https://horizon.netscout.com/

30 útoků za 3 měsíce

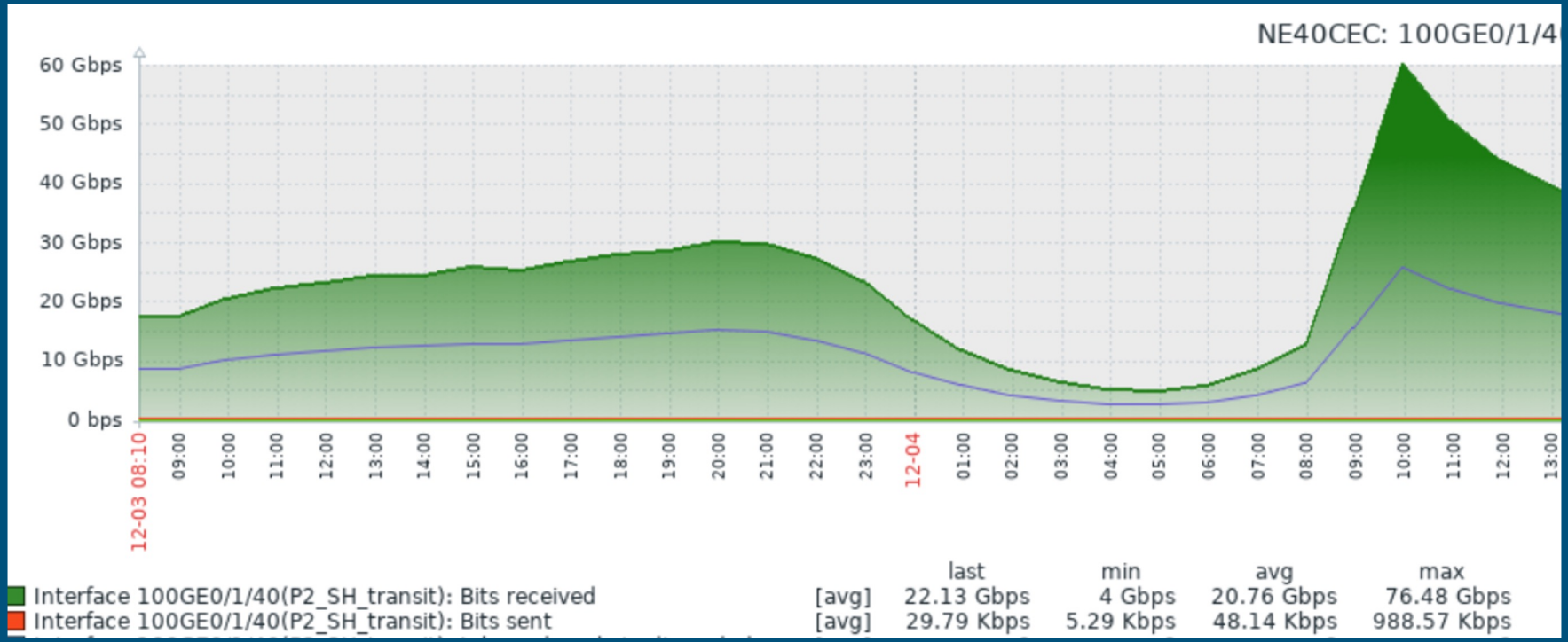
Byl detekován DDOS útok z IP 217.7	6.6.2023 17:42
Byl detekován DDOS útok na IP 185	6.6.2023 11:55
Byl detekován DDOS útok na IP 45.'	24.5.2023 18:18
Byl detekován DDOS útok na IP 45.'	24.5.2023 18:03
Byl detekován DDOS útok na IP 45.'	24.5.2023 17:39
Byl detekován DDOS útok na IP 185	24.5.2023 8:47
Byl detekován DDOS útok z IP 217.7	24.5.2023 1:17
Byl detekován DDOS útok na IP 217	18.5.2023 13:01
Byl detekován DDOS útok na IP 185	5.5.2023 19:50
Byl detekován DDOS útok na IP 185	5.5.2023 19:36
Byl detekován DDOS útok na IP 185	5.5.2023 19:24
Byl detekován DDOS útok na IP 185	5.5.2023 19:07
Byl detekován DDOS útok na IP 185	5.5.2023 18:52
Byl detekován DDOS útok na IP 185	5.5.2023 18:32

Byl detekován DDOS útok na IP 45.'	30.4.2023 18:09
Byl detekován DDOS útok na IP 185	29.4.2023 14:14
Byl detekován DDOS útok z IP 217.7	17.4.2023 15:52
Byl detekován DDOS útok z IP 217.7	16.4.2023 14:02
Byl detekován DDOS útok na IP 37.2	13.4.2023 22:50
Byl detekován DDOS útok na IP 185	5.4.2023 19:04
Byl detekován DDOS útok na IP 185	30.3.2023 0:24
Byl detekován DDOS útok na IP 37.2	29.3.2023 19:33
Byl detekován DDOS útok na IP 37.2	29.3.2023 0:30
Byl detekován DDOS útok na IP 37.2	26.3.2023 18:11
Byl detekován DDOS útok na IP 45.'	26.3.2023 18:04
Byl detekován DDOS útok na IP 37.2	26.3.2023 17:57
Byl detekován DDOS útok na IP 37.2	26.3.2023 17:01
Byl detekován DDOS útok na IP 37.2	26.3.2023 15:24
Byl detekován DDOS útok na IP 37.2	26.3.2023 14:29
Byl detekován DDOS útok na IP 37.2	24.3.2023 19:41

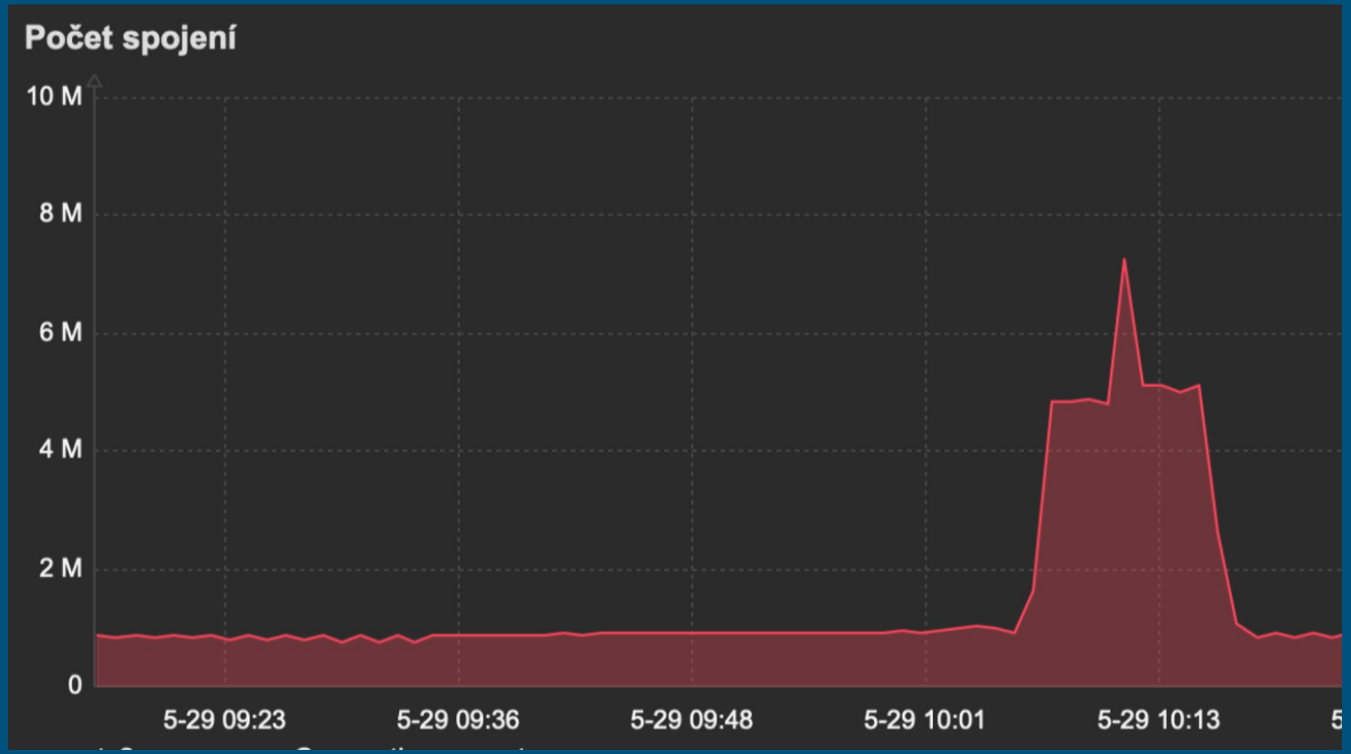
Byl detekován DDOS útok na IP 37.2	20.3.2023 22:55
Byl detekován DDOS útok na IP 37.2	20.3.2023 18:15
Byl detekován DDOS útok na IP 37.2	20.3.2023 18:00
Byl detekován DDOS útok na IP 37.2	20.3.2023 17:45
Byl detekován DDOS útok na IP 37.2	20.3.2023 16:56
Byl detekován DDOS útok na IP 37.2	20.3.2023 16:02
Byl detekován DDOS útok na IP 37.2	20.3.2023 15:50
Byl detekován DDOS útok na IP 37.2	19.3.2023 19:24
Byl detekován DDOS útok na IP 37.2	19.3.2023 18:57
Byl detekován DDOS útok na IP 37.2	19.3.2023 17:56
Byl detekován DDOS útok na IP 37.2	19.3.2023 17:37
Byl detekován DDOS útok na IP 37.2	19.3.2023 17:20
Byl detekován DDOS útok na IP 37.2	19.3.2023 16:29
Byl detekován DDOS útok na IP 37.2	19.3.2023 10:37

Byl detekován DDOS útok na IP 37.2	19.3.2023 8:15
Byl detekován DDOS útok na IP 37.2	19.3.2023 1:14
Byl detekován DDOS útok na IP 37.2	19.3.2023 0:00
Byl detekován DDOS útok na IP 37.2	18.3.2023 23:33
Byl detekován DDOS útok na IP 37.2	18.3.2023 20:52
Byl detekován DDOS útok na IP 37.2	18.3.2023 16:26
Byl detekován DDOS útok na IP 37.2	18.3.2023 16:00
Byl detekován DDOS útok na IP 37.2	17.3.2023 17:51
Byl detekován DDOS útok na IP 45.'	17.3.2023 14:00
Byl detekován DDOS útok na IP 37.2	15.3.2023 15:06
Byl detekován DDOS útok na IP 37.2	15.3.2023 14:53
Byl detekován DDOS útok na IP 37.2	14.3.2023 21:18
Byl detekován DDOS útok na IP 37.2	12.3.2023 20:19

TOP útok 100 Gbps



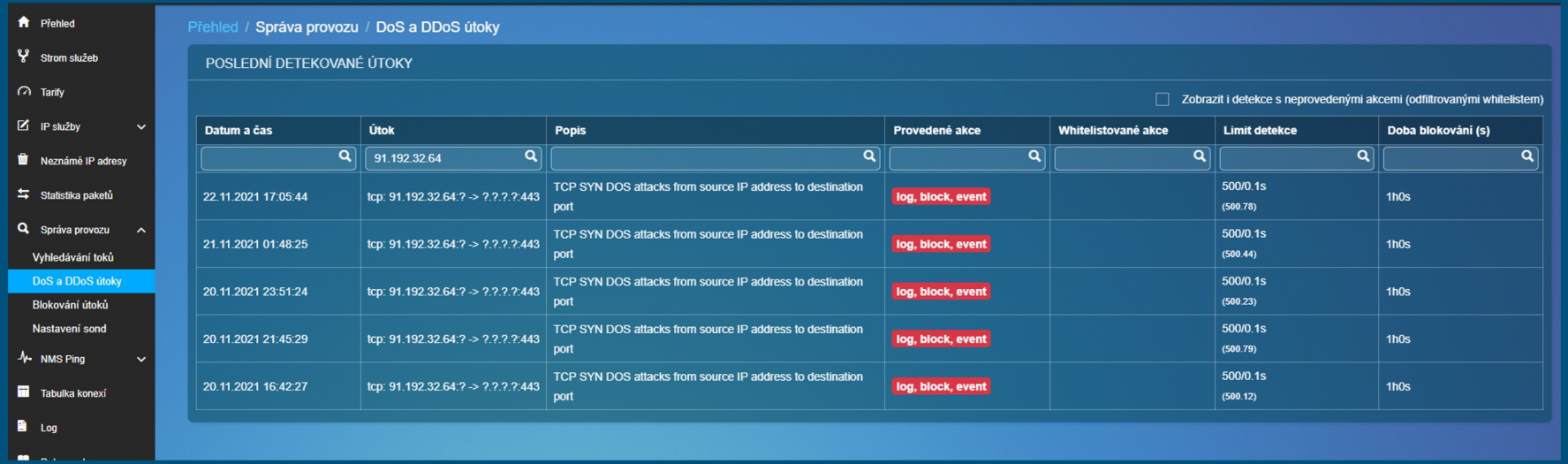
Zdroj nemusí být zvenčí



Zdroj nemusí být zvenčí

START TIME - FIRST SEEN	TRVÁNÍ	PROTOKOL	ZDROJOVÁ IP ADRESA	ZDROJOVÝ PORT	CÍLOVÁ IP ADRESA	CÍLOVÝ PORT	TCP PŘÍZNAKY	TOS	PAKETY	BAJTY	TOKY
2023-05-29 10:05:12.199	0.02 s	TCP	u1[illegible].cz	34265	vps-a8fa4974.vps.ovh.ca	46561	....A....	Best Effort & Default	2	2.83 KB	1
2023-05-29 10:05:12.841	0.012 s	TCP	u1.cz	53591	vps-a8fa4974.vps.ovh.ca	48580	....A....	Best Effort & Default	2	2.83 KB	1
2023-05-29 10:05:12.056	0 s	TCP	u1.cz	56414	vps-a8fa4974.vps.ovh.ca	53603	....A....	Best Effort & Default	2	2.83 KB	1
2023-05-29 10:05:12.224	0.001 s	TCP	u1.cz	52920	vps-a8fa4974.vps.ovh.ca	23374	....A....	Best Effort & Default	2	2.83 KB	1
2023-05-29 10:05:11.811	0 s	TCP	u1.cz	16215	vps-a8fa4974.vps.ovh.ca	21444	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:11.986	0 s	TCP	u1.cz	40682	vps-a8fa4974.vps.ovh.ca	bpcp-poll	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:12.135	0 s	TCP	u1[illegible].cz	40573	vps-a8fa4974.vps.ovh.ca	gpsd	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:12.525	0 s	TCP	u1.cz	62018	vps-a8fa4974.vps.ovh.ca	26427	....A....	Best Effort & Default	2	2.83 KB	1
2023-05-29 10:05:11.427	0 s	TCP	u1.cz	14828	vps-a8fa4974.vps.ovh.ca	16694	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:11.731	0 s	TCP	u1[illegible].cz	32135	vps-a8fa4974.vps.ovh.ca	56568	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:12.256	0 s	TCP	u1.cz	13375	vps-a8fa4974.vps.ovh.ca	knet-cmp	....A....	Best Effort & Default	2	2.83 KB	1
2023-05-29 10:05:12.456	0 s	TCP	u1.cz	29258	vps-a8fa4974.vps.ovh.ca	26939	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:12.006	0 s	TCP	u1.cz	zigbee-ip	vps-a8fa4974.vps.ovh.ca	7519	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:13.054	0 s	TCP	u1[illegible].cz	40758	vps-a8fa4974.vps.ovh.ca	14793	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:12.135	0 s	TCP	u1.cz	9120	vps-a8fa4974.vps.ovh.ca	20275	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:13.063	0 s	TCP	u1.cz	15520	vps-a8fa4974.vps.ovh.ca	40872	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:11.789	0 s	TCP	u1.cz	49400	vps-a8fa4974.vps.ovh.ca	21889	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:13.225	0 s	TCP	u1.cz	32218	vps-a8fa4974.vps.ovh.ca	61159	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:11.731	0 s	TCP	u1.cz	10780	vps-a8fa4974.vps.ovh.ca	13574	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:13.144	0 s	TCP	u1.cz	38227	vps-a8fa4974.vps.ovh.ca	60066	....A....	Best Effort & Default	2	2.83 KB	1
2023-05-29 10:05:13.337	0 s	TCP	u1[illegible].cz	21839	vps-a8fa4974.vps.ovh.ca	62512	....A....	Best Effort & Default	2	2.83 KB	1
2023-05-29 10:05:13.516	0 s	TCP	u1.cz	57165	vps-a8fa4974.vps.ovh.ca	19568	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:11.174	0 s	TCP	u1.cz	52425	vps-a8fa4974.vps.ovh.ca	55224	....A....	Best Effort & Default	1	1.42 KB	1
2023-05-29 10:05:12.574	0 s	TCP	u1[illegible].cz	45069	vps-a8fa4974.vps.ovh.ca	55685	....A....	Best Effort & Default	2	2.83 KB	1

Utněme to na začátku



Ochrana a řešení

- kontrola otevřených portů - minimálně NTP a DNS
- BCP38
- RTBH
- BGP Flowspec
- čištění provozu
- spolupráce s upstreamem

INTERNET

Router

NetFlow
SFlow
Mirroring
Tapping

RTBH
Flowspec
ReRouting

ANALÝZA PROVOZU

VYVOLÁNÍ AKCE